UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/068,280	02/04/2002	Mark J. McArdle	01.239.01	9739

7590 12/12/2008

ZILKA-KOTAB PC
PO Box 721120
San Jose, CA 95172-1120

EXAMINER	
TRUVAN, LEYNNA THANH	

ART UNIT	PAPER NUMBER
2435	

MAIL DATE	DELIVERY MODE
12/12/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte MARK J. MCARDLE and BRENT A. JOHNSTON

Appeal 2007-4302
Application 10/068,280[1]
Technology Center 2100

Decided: December 12, 2008

Before LANCE LEONARD BARRY, ALLEN R. MACDONALD, and CAROLYN D. THOMAS, *Administrative Patent Judges.*

THOMAS, *Administrative Patent Judge.*

DECISION ON APPEAL

I. STATEMENT OF THE CASE

Appellants appeal under 35 U.S.C. § 134 from a final rejection of claims 1-51 mailed November 15, 2005, which are all the claims remaining in the application. We have jurisdiction under 35 U.S.C. § 6(b).

We affirm-in-part.

---

[1] Application filed February 4, 2002. The real party in interest is McAfee, Inc.

A. INVENTION

Appellants invented a system, method, and computer readable medium for providing intrusion prevention for a computer based on intrusion rules corresponding to active networked applications executing on the computer. The intrusion rules are a subset of a full rule set that may include signatures of known attacks or heuristic rules. The subset changes as network connections for active applications are initiated and terminated, or as the active applications terminate. (Spec., Abstract.)

B. ILLUSTRATIVE CLAIM

The appeal contains claims 1-51. Claims 1, 15, 29, and 43 are independent claims. Claim 1 is illustrative:

1. A computerized method comprising:

determining an active networked application;

filtering a set of intrusion rules to create a subset of intrusion rules corresponding to the active networked application, where the subset of the intrusion rules corresponding to the active networked application are capable of being used for evaluating intrusions that target the corresponding active networked application; and

evaluating network traffic using the subset of intrusion rules;

wherein the subset of the intrusion rules corresponding to the active networked application are used for the evaluation for reducing a required amount of processing resources.

C. REFERENCES

The references relied upon by the Examiner in rejecting the claims on appeal are as follows:

Freund	US 5,987,611	Nov. 16, 1999
Kaler	US 6,671,829 B2	Dec. 30, 2003
Hanko	US 6,912,578 B1	Jun. 28, 2005

D. REJECTIONS

The Examiner entered the following rejections which are before us for review:

(1) Claims 1-4, 7-12, 14-18, 21-26, 28-32, 35-40, 42-44, 47, 48, 50 and 51 rejected under 35 U.S.C. § 103(a) as being unpatentable over Freund in view of Kaler;

(2) Claims 13, 27, 41, and 49 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Freund, Kaler in view of Official Notice; and

(3) Claims 5, 6, 19, 20, 33, 34, 45, and 46 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Freund, Kaler in view of Hanko.

II. PROSECUTION HISTORY

Appellants appealed from the Final Rejection and filed an Appeal Brief (App. Br.) on June 12, 2006. The Examiner mailed an Examiner's Answer (Ans.) on September 11, 2006. Appellants filed a Reply Brief (Reply Br.) on November 13, 2006.

III. FINDINGS OF FACT

The following findings of fact (FF) are supported by a preponderance of the evidence.

Freund

1. Freund discloses "system and methods for regulating access and maintaining security of individual computer systems." (Col. 1, ll. 25-27.)

2. Freund discloses that "a whole new set of challenges face LAN administrators and individual users alike . . . (1) attacks by perpetrators (hackers) capable of damaging the local computer systems, misuse these systems or steal proprietary data and programs . . . (3) infiltration by viruses and 'Trojan Horse' programs . . . ." (Col. 1, l. 66 to col. 2, l. 9.)

3. Freund discloses "one or more access management applications that set access rules for the entire LAN for one or more workgroups or individual users, a client-based filter application . . ." (Col. 3, ll. 61-64.)

4. Freund discloses "keeping a list of currently active processes; intercepting certain keyboard, mouse and other interactive user activities in order to determine which process is actively used." (Col. 4, ll. 32-35.)

5. Freund discloses that "[b]y intercepting process loading and unloading and keeping a list of currently active processes, each client process can be checked for various characteristics . . . ." (Col. 4, ll. 40-42.)

6. Freund discloses "a supervisor process, which specifies rules which govern Internet access by the client computers including the particular client computer . . .[t]ransmitting a filtered subset of the rules to the particular client computer." (Col. 5, ll. 38-43.)

7. Freund discloses that "[i]f application is not allowed to access the Internet or not allowed to use the specific protocol then client monitor can stop application from accessing the Internet." (Col. 5, ll. 61-63.)

8. Freund discloses that "access rules can include criteria such as . . . a list of applications or application versions that a user can or cannot use . . . a list of protocols . . . ." (Col. 4, ll. 8-19.)

Kaler

9. Kaler discloses a method and apparatus that "provides a system user with tools for analyzing an application running thereon . . . without modifying it or degrading its performance or data security characteristics." (Abstract.)

10. Kaler discloses that "[t]he developer can specify by means of a 'filter' what to look for in the system under examination." (Col. 4, ll. 17-18.)

11. Kaler discloses that "the invention provides suitable data security mechanisms throughout the network being monitored. Discretionary access is applied to the collection of data from a specific machine." (Col. 5, ll. 27-30.)

IV. PRINCIPLES OF LAW

Obviousness

"What matters is the objective reach of the claim. If the claim extends to what is obvious, it is invalid under § 103." *KSR Int'l Co. v. Teleflex, Inc.*, 127 S. Ct. 1727, 1742 (2007). To be nonobvious, an improvement must be "more than the predictable use of prior art elements according to their established functions." *Id.* at 1740.

Appellants have the burden on appeal to the Board to demonstrate error in the Examiner's position. See *In re Kahn*, 441 F.3d 977, 985-86 (Fed. Cir. 2006) ("On appeal to the Board, an applicant can overcome a rejection [under § 103] by showing insufficient evidence of prima facie obviousness or by rebutting the *prima facie* case with evidence of secondary indicia of nonobviousness.") (quoting *In re Rouffet*, 149 F.3d 1350, 1355 (Fed. Cir. 1998)). Therefore, we look to Appellants' Brief to show error in the proffered prima facie case. Only those arguments actually made by Appellants have been considered in this decision. Arguments which Appellants could have made but chose not to make in the Brief have not been considered and are deemed to be waived. *See* 37 C.F.R. § 41.37(c)(1)(vii).

"Section 103 forbids issuance of a patent when 'the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains.'" *KSR Int'l Co. v. Teleflex Inc.*, 127 S. Ct. 1727, 1734 (2007). The question of obviousness is resolved on the basis of underlying factual determinations including (1) the scope and content of the prior art, (2) any differences between the claimed subject matter and the prior art, (3) the level of skill in the art, and (4) where in evidence, so-called secondary considerations. *Graham v. John Deere Co.*, 383 U.S. 1, 17-18 (1966). *See also KSR*, 127 S. Ct. at 1734 ("While the sequence of these questions might be reordered in any particular case, the [*Graham*] factors continue to define the inquiry that controls.")

Non-Analogous Art

The analogous-art test requires that the Board show that a reference is either in the field of the Applicant's endeavor or is reasonably pertinent to the problem with which the inventor was concerned in order to rely on that reference as a basis for rejection. *In re Oetiker*, 977 F.2d 1443, 1447 (Fed. Cir. 1992). References are selected as being reasonably pertinent to the problem based on the judgment of a person having ordinary skill in the art. *Id.* ("[I]t is necessary to consider 'the reality of the circumstances,'-in other words, common sense-in deciding in which fields a person of ordinary skill would reasonably be expected to look for a solution to the problem facing the inventor." (quoting *In re Wood*, 599 F.2d 1032, 1036 (CCPA 1979))). *In re Kahn*, 441 F.3d 977, 986-87 (Fed. Cir. 2006).

V. ANALYSIS

Grouping of Claims

Group I: In the Brief, Appellants argue claims 1, 7-15, 21-29, 35-43, 47, 49, and 50 as a group (App. Br. 10-16). For claims 7-15, 21-29, 35-43, 47, 49, and 50, Appellants repeat the same argument made for claim 1. We will, therefore, treat claims 7-15, 21-29, 35-43, 47, 49, and 50 as standing or falling with claim 1.

Group II: Appellants essentially argue claims 2-4, 16-18, 30-32, and 44 as a group (App. Br. 16). For claims 3, 4, 16-18, 30-32, and 44, Appellants essentially repeat the same argument made for claim 2. We will, therefore, treat claims 3, 4, 16-18, 30-32, and 44 as standing or falling with claim 2.

Group III: Appellants argue claims 5, 6, 19, 20, 33, 34, 45, and 46 as a group (App. Br. 17). For claims 6, 19, 20, 33, 34, 45, and 46, Appellants repeat the same argument made for claim 5. We will, therefore, treat claims 6, 19, 20, 33, 34, 45, and 46 as standing or falling with claim 5.

Group IV: Appellants separately argue claim 48 (App. Br. 17).

Group V: Appellants separately argue claim 51 (App. Br. 17-18).

See 37 C.F.R. § 41.37(c)(1)(vii). *See also In re Young*, 927 F.2d 588, 590 (Fed. Cir. 1991).

The Obviousness Rejection

We now consider the Examiner's rejection of claims 1-51 under 35 U.S.C. § 103(a).

Group I
Claims 1, 7-15, 21-29, 35-43, 47, 49, and 50

Missing Feature Argument

Appellants contend that in Freund "the client based filter application and the Client Monitor [that] compar[es] application properties with a database of applications allowed to access the internet simply fails to meet '<u>filtering a set of intrusion rules</u> to create <u>a subset of intrusion rules</u> **<u>corresponding to the active networked application</u>**.'" (App. Br. 13; see also Reply Br. 9-11.) Appellants further contend that "Kaler does <u>not</u> teach a subset of <u>intrusion rules</u>, as claimed by appellant[s], but instead only teaches a filter that collects events for specified items." (App. Br. 16.)

The Examiner found that in Freund "[t]he filtering application involves monitoring, logging, and filtering work (col. 3, lines 51-52 and col. 4, lines 29-32). Freund discloses filtering as the ability to monitor and regulate Internet access on a per application basis by determining which applications can/cannot access the Internet." (Ans. 27.)

Issue: Have Appellants shown that the Examiner erred in equating Freund's Client Monitoring method with filtering a set of intrusion rules to create a subset of intrusion rules corresponding to the active networked application?

Freund discloses a system and method that regulates access to the Internet (FF 1). Freund's system looks at challenges posed by attacks from perpetrators trying to damage the local computer systems and includes access management applications that set access rules so as to try to combat such attacks (FF 2-3). Freund determines which applications are active (FF 4) and checks each active process for various characteristics (FF 5) using a filtered subset of rules transmitted to that particular client computer (FF 6).

In other words, Freund discloses rules and subset of rules for regulating access to the Internet for each process/application on a particular computer. Similarly, Kaler discloses providing a system user with tools for analyzing an application running thereon (FF 9) and using a filter to specify what to look for in the system under examination (FF 10).

Thus, we find that Freund and Kaler teaches and reasonably suggests the claimed "filtering a set of intrusion rules to create a subset of intrusion rules corresponding to the active networked application."

Non-Analogous Art Argument

Appellants contend that "[t]o simply glean features from a security system, such as that of Freund, and combine the same with the *non-analogous art* of a performance analyzer, such as that of Kaler, would simply be improper." (App. Br. 10; see also Reply Br. 6.) Appellants further contend that "Kaler's disclosure that flow and performance information can be specified, captured, and analyzed, without degrading its data security characteristics *teaches away* from any sort of security system, contrary to the Examiner's assertion that Kaler 'comprises security prevention.'" (App. Br. 11: see also Reply Br. 6.)

The Examiner found that "it would have been obvious for a person of ordinary skills in the art to combine the teaching the subset of intrusion rules of Freund with the teaching of filter reduction to extract only the information of interest as taught by Kaler because this reduces the performance impact of monitoring." (Ans. 5.)

Issue: Have Appellants shown that Kaler is non-analogous art to Freund and that the Examiner erred in combining Kaler with Freund?

While strict insistence on identifying a suggestion to modify the prior art is inimical to Supreme Court precedent concerning obviousness (*KSR*, 127 S. Ct. at 1741), we find that Kaler provides a suggestion to modify Freund that would have been considered by a person of ordinary skill in the art. For instance, Appellants sought to provide intrusion prevention for a computer based on intrusion rules corresponding to an active networked application executing on the computer (Spec., Abstract). Kaler teaches providing tools for analyzing an application running on a system without degrading its data security characteristics (FF 9) and filtering what to look

for in the system (FF 10). Thus, Kaler teachings apply to the very application specific problems that Appellants' sought to solve and are at least "reasonably pertinent" to a person of ordinary skill in the art. *In re Kahn*, 441 F.3d 977, 986-87 (Fed. Cir. 2006). Further supporting this conclusion is that fact that Kaler discloses that its invention provides suitable data security mechanisms (FF 11). Thus, we find that it would have been obvious to apply the teachings of Kaler to the Internet access management system of Freund so as to reduce the performance impact of monitoring.

Therefore, we do *not* find that Appellants have shown error in the Examiner's rejection of illustrative claim 1. Instead, we find the Examiner has set forth a sufficient initial showing of obviousness. Appellants have not shown that the combination of Freund and Kaler lacks the above-noted disputed features of claim 1 *or* that it is improper to combine the two references. Therefore, we affirm the rejection of independent claim 1 and of claims 7-15, 21-29, 35-43, 47, 49, and 50, which fall therewith.

Group II
Claims 2-4, 16-18, 30-32, and 44

Appellants contend that "Freund simply fails to even suggest a situation where an 'active networked application becomes inactive' (emphasis added), and especially does not teach that, when such occurs, 'the set of intrusion rules [are re-filtered],' as claimed by appellant[s]." (App. Br. 16.) Appellants contend that "stopping a client from accessing the Internet, as disclosed by Freund, fails to meet 'detecting when the active networked application becomes inactive.'" (Reply Br. 23.)

The Examiner found that "Freund discloses detecting when the active networked application becomes inactive is when there are violated rules for the attempt to access the Internet because the communication is terminated or stops the application [sic] from accessing the Internet." (Ans. 33.)

Issue: Have Appellants shown that the Examiner erred in finding that Freund discloses "detecting when the active networked application becomes inactive, and if so, re-filtering the rules?"

The Examiner has presented us with a teaching of Freund that discloses that if an application is not allowed to access the Internet the client monitor can stop the application. (Ans. 33; FF 7.) Here, the Examiner seems to suggest that stopping the application is the same as detecting when the application becomes inactive. We find the Examiner's reasoning to show "connection terminations" which arguably reads on "becoming inactive." Further, we find that Freund *clearly* discloses that its monitoring duties include keeping a list of currently active processes (FF 4-5). Here, it goes to follow that in order to keep such an "active" list, one must be able to detect when applications become inactive so as to update the list. Thus, we find that Freund's list of active applications "reasonably suggests" detecting when the active networked application becomes inactive, i.e., so as to remove it from the list. Freund further notes that by keeping the list of currently active processes, each process can be checked for various characteristics, i.e., in essence a re-filtering of the rules.

Therefore, we do *not* find that Appellants have shown error in the Examiner's rejection of illustrative claim 2. Instead, we find the Examiner has set forth a sufficient initial showing of obviousness. Therefore, we affirm the rejection of claim 2 and of claims 3, 4, 16-18, 30-32, and 44, which fall therewith.

Group III
Claims 5, 6, 19, 20, 33, 34, 45, and 46

Appellants contend that the portions of Freund cited by the Examiner "only relate to 'prescribed remedial action for any violated rule' such that 'the communication is. . . terminated.' Clearly, terminating a communication upon detection of a rule violation, as in Freund, does not even remotely relate to appellant's claim language." (App. Br. 17.)

Appellants contend that "the mere disclosure of stopping a program when user interaction stops, when there is no chance of user input, and no need for user output simply fails to even suggest 'detecting when no network application is active; and suspending the evaluating of network traffic until a networked application is active.'" (Reply Br. 28.)

Appellants contend that "Freund relates to a security system, while Hanko relates to improving resource utilization on a shared client. To simply glean features from a security system, such as that of Freund, and combined the same with the *non-analogous art* of improving utilization on a shared client system, such as that of Hanko, would simply be improper." (Reply Br. 26.)

The Examiner found that Hanko discloses "a mechanism to stop a program from consuming resources when it detects a user has stopped interaction with an application and to restart it when the user begins interaction with it." (Ans. 14.)

Issue: Have Appellants shown that the Examiner erred in finding that Hanko discloses detecting when *no* networked application is active and suspending the evaluating of network traffic until a networked application is active?

The Examiner seems to suggest (e.g., Ans. 14) that the first paragraph of claim 5 is taught by Hanko's "causing an application to stop consuming a resource" features. We cannot say that there are not any *"detecting when no networked application is active"* feature in the prior art that operate in a fashion analogous to that required by the claim. We can only rule on the basis of the evidence that is provided in support of the rejection, and we find it deficient here. The allocation of burdens requires that the USPTO produce the factual basis for its rejection of an application under 35 U.S.C. §§ 102 and 103. *In re Piasecki*, 745 F.2d 1468, 1472 (Fed. Cir. 1984) (citing *In re Warner*, 379 F.2d 1011, 1016 (CCPA 1967)). The one who bears the initial burden of presenting a prima facie case of unpatentability is the Examiner. *In re Oetiker*, 977 F.2d 1443, 1445 (Fed. Cir. 1992).

In this case, we find that the Examiner's evidence at most shows detecting inactivity amongst applications. However, the representative claim 5 requires *"detecting when no networked application is active; and suspending the evaluating of networked traffic until a networked application*

is active." Claim 6 recites similar features regarding continuing the evaluating . . . is no networked application is active. The Examiner has not shown and we do not readily find these features in the cited art.

Therefore, we find that Appellants have shown error in the Examiner's rejection of illustrative claim 5. Therefore, we reverse the rejection of claim 5 and of claims 6, 19, 20, 33, 34, 45, and 46, which stand therewith.

Group IV
Claim 48

Appellants contend that "such information associated with the rules as taught in Freund only relate to the application of the rules, and not to the substance of the rules including 'a targeted active networked application, a specified hostile payload, a network port, and a protocol,' as specifically claimed by appellant[s]." (App. Br. 17; see also Reply Br. 29-30.)

The Examiner found that "Freund discloses monitoring access to the Internet by individual applications allows the system to not only track Internet traffic but also can determine data exchanges on a per application basis including the ability to determine the name of individual files downloaded as well as target directories to where such files are copied." (Ans. 35.)

Issue: Have Appellants shown that the Examiner erred in finding that Freund discloses intrusion rules that include information selected from the group consisting of a target active networked application, a specific hostile payload, a network port, and a protocol?

The Examiner found that Freund's system can create an audit trail to track data exchange on a per application basis (Ans. 35). In doing so, Freund discloses that the access rules include certain criteria including a list of applications that can be used and a list of protocols (FF 8). We find that the claimed *"wherein the intrusion rules include information selected from the group consisting of a target active networked application, a specific hostile payload, a network port, and a protocol"* reads on Freund's access rules criteria that include at least a list of applications and protocols that can be used. Claim 48 does not require that all the items in the group be included in the information, only that the intrusion rules include information selected from the group.

Therefore, we do *not* find that Appellants have shown error in the Examiner's rejection of illustrative claim 48. Instead, we find the Examiner has set forth a sufficient initial showing of obviousness. Therefore, we affirm the rejection of claim 48.

Group V
Claim 51

Appellants contend that the portions of Freund cited by the Examiner "do not even suggest any sort of heuristic rule, as claimed by appellant[s]. Second, only determining which applications are actively used by a user, as in Freund, clearly does not meet any sort of 'information associated with an active networked application making a new connection never previously made,' as specifically claimed by appellant[s]." (App. Br. 18; see also Reply Br. 31.)

The Examiner found that "Freund discloses the application panel displays a new mode for indicating the new executing process and each driver is responsible for monitoring and filtering access for its particular type, including ensuring that any user activity which employs that access type conforms to any rules or conditions specified." (Ans. 35-36.)

Issue: Have Appellants shown that the Examiner erred in finding that Freund discloses a heuristic rule that includes information associated with an active application making a new connection never previously made?

The Examiner found that Freund discloses a panel for indicating a new executing process and that such a display conforms to rules or conditions specified for the Internet monitor (Ans. 35-36). Claim 51 requires that the heuristic rule includes information associated with an active networked application making a new connection never previously made. We find that Freund's displaying of a *new* executing process (e.g., application) *reasonably suggests* information associated with an active networked application making a new connection never previously made. Furthermore, Appellants merely argue that neither reference teaches or suggests heuristic rules without providing any meaningful analysis that explains why the Examiner's proffered findings are in error. (App. Br. 18.) A statement which merely points out what a claim recites will not be considered an argument for separate patentability of the claim. *See* 37 C.F.R. § 41.37(c)(1)(vii).

Therefore, we do *not* find that Appellants have shown error in the Examiner's rejection of illustrative claim 51. Instead, we find the Examiner has set forth a sufficient initial showing of obviousness. Therefore, we affirm the rejection of claim 51.

VI. CONCLUSIONS

We conclude that Appellants have *not* shown that the Examiner erred in rejecting claims 1-4, 7-18, 21-32, 35-44, and 47-51.

We conclude that Appellants have shown that the Examiner erred in rejecting claims 5, 6, 19, 20, 33, 34, 45 and 46.

VII. DECISION

In view of the foregoing discussion,

(1) We affirm the Examiner's rejection of claims 1-4, 7-18, 21-32, 35-44, and 47-51; and

(2) We reverse the Examiner's rejection of claims 5, 6, 19, 20, 33, 34, 45, and 46.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a). *See* 37 C.F.R. § 1.136(a)(1)(iv) (2007).

AFFIRMED-IN-PART

pgc

ZILKA-KOTAB PC
PO Box 721120
San Jose CA 95172-1120